Copy for the designated Office (DO/US) PCT/EP99/06344

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

DE VRIES & METMAN B.V.
Overschiestraat 180
NL-1062 XK Amsterdam
PAYS-BAS

Date of mailing (day/month/year) 29 March 2000 (29.03.00)	
Applicant's or agent's file reference WO2923-dV	**IMPORTANT NOTIFICATION**
International application No. PCT/EP99/06344	**International filing date** (day/month/year) 30 August 1999 (30.08.99)

1. The following indications appeared on record concerning:

[ ] the applicant [ ] the inventor [X] the agent [ ] the common representative

Name and Address

DE VRIES & METMAN B.V.
Gebouw Autumn
Overschiestraat 184 N
NL-1062 XK Amsterdam
Netherlands

State of Nationality:

State of Residence:

Telephone No.: +31 20 6694432

Facsimile No.: +31 20 6694516

Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [ ] the name [X] the address [ ] the nationality [ ] the residence

Name and Address

DE VRIES & METMAN B.V.
Overschiestraat 180
NL-1062 XK Amsterdam
Netherlands

State of Nationality:

State of Residence:

Telephone No.: 020 511 0930

Facsimile No.: 020 511 0931

Teleprinter No.:

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[ ] the International Preliminary Examining Authority
[X] the designated Offices concerned
[ ] the elected Offices concerned
[ ] other:

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland** Facsimile No.: (41-22) 740.14.35	Authorized officer C. Cupello Telephone No.: (41-22) 338.83.38

Form PCT/IB/306 (March 1994) 003195957

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 06 September 2000 (06.09.00)	
International application No. PCT/EP99/06344	**Applicant's or agent's file reference** WO2923-dV
International filing date (day/month/year) 30 August 1999 (30.08.99)	**Priority date** (day/month/year) 31 August 1998 (31.08.98)
Applicant MOOIJ, Wilhelmus, Gerardus, Petrus et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

21 February 2000 (21.02.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Nestor Santesso

Telephone No.: (41-22) 338.83.38

09176373Z

PATENT COOPERATION TREATY

REC'D 12 DEC 2000
WIPO PCT

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

3

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
WO2923-dV/jdh		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP99/06344	30/08/1999	31/08/1998
International Patent Classification (IPC) or national classification and IPC G06F1/00		
Applicant IRDETO ACCESS B.V.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 4 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 6 sheets.

   7

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
21/02/2000	08.12.2000
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Van de Maele, L Telephone No. +49 89 2399 8805

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/EP99/06344

I. Basis of the report

1. This report has been drawn on the basis of *(substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments (Rules 70.16 and 70.17).)*:
Description, pages:

4-8	as originally filed	
1-3	with telefax of	06/11/2000

Claims, No.:

1-15	with telefax of	06/11/2000

Drawings, sheets:

1/3-3/3	as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   - ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
   - ☐ the language of publication of the international application (under Rule 48.3(b)).
   - ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   - ☐ contained in the international application in written form.
   - ☐ filed together with the international application in computer readable form.
   - ☐ furnished subsequently to this Authority in written form.
   - ☐ furnished subsequently to this Authority in computer readable form.
   - ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   - ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-8,10-15
	No:	Claims	9
Inventive step (IS)	Yes:	Claims	1-8,10-15
	No:	Claims	9
Industrial applicability (IA)	Yes:	Claims	1-8,10-15
	No:	Claims	9

2. Citations and explanations
   see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

ANNEX TO SECTIONS V AND VIII

1. Claim 5 should be dependent upon claim 4 rather than on claim 3 because at present there is no antecedent for the virtual machine referred to in claim 5. It is assumed that this error is merely based on a typing mistake.

2. Claim 9 appears to be inconsistent with the claims it depends upon. According to claim 9, the secure device applet is downloaded from a network whereas according to the other claims it is included in the protocol information delivered with the protected contents. Therefore, claim 9 does not comply with Article 6 PCT and no positive statement in respect of Article 33 PCT can be made.

ANNEX TO SECTION VII

1. The independent claims are not drafted in the two-part form in accordance with Rule 6.3(b) PCT. Such two-part form should have reflected the prior art features known from the document cited in the opening part of the description (page 1).

WO 2923-dV/jdh

System for providing encrypted data, system for decrypting encrypted data and method for providing a communication interface in such a decrypting system.

The invention generally relates to a system for providing encrypted data to be used in a content player, to a system for decrypting encrypted data in a content player, and to a method for providing a communication interface between a decryption device and a secure device in a content player. More particularly the invention relates to such systems and a method to create an open access interface for a wide range of multimedia terminals.

In the present specification the term "content player" is meant to indicate any type of consumer equipment, such as a (digital) TV set, a set top box, a DVD player or a (digital) VCR. In order to allow access to contents, such as a movie, football match, etc., it is known to protect the contents by encryption of the data using a suitable encryption algorithm. Subscribers are provided with a set top box for example and a secure device, wherein the secure device generates information necessary to decrypt the encrypted data. Conventional systems of this type are provided with a fixed interface and protocols for communication between the secure device and the content player. A fixed interface shows the disadvantage that the content player can only be used with one or more specific secure devices. <..>

The invention aims to provide systems and a method of the above-mentioned type allowing to create a variable interface between the secure device and a content player.

According to a first aspect of the invention, a system for providing encrypted data to be used in ~~the~~ a content

<EP-A-0 750 423 discloses a conditional access module cooperating with a smart card as secure device through a fixed interface.>

according to claim 1

player is provided. ~~Comprising an encryption device for encrypting data using an encryption algorithm, a protection device for providing secure device data, and for providing information on a protocol for communication between the content player and a secure device, and a control device for providing a protected contents containing the encrypted data, the secure device data, said protocol information and attribute data on the different parts inside the protected contents.~~

According to a second aspect of the invention, a system for decrypting encrypted data in a content player according to claim 3 is provided. ~~Comprising an input for receiving a protected contents containing the encrypted data, secure device data, information on a protocol for communication between the content player and a secure device, and attribute data on the different parts inside the protected contents, a decryption device and a control device, wherein the control device is programmed to use said protocol information to establish a communication interface between the decryption device and a secure device used with the contents player, wherein the decryption device is adapted to communicate with the secure device as controlled by the protocol information to obtain information required to decrypt the encrypted data.~~

According to a further aspect of the invention, a method for providing a communication interface between a decryption device in a content player and a secure device according to claim 10 is provided. ~~Comprising receiving a protected contents containing information on a protocol for communication between the content player and a secure device, and attribute data on the different parts inside the protected contents, retrieving said protocol information from the protected contents to establish a communication interface between the decryption device and a secure device used with the contents player.~~

According to a still further aspect of the invention a method ~~for transmitting or the like of encrypted data~~ according to claim 15 is provided. ~~Wherein the encrypted data is obtained by means of the system for providing encrypted data according to the invention.~~

In this manner the invention provides a variable interface platform, wherein any communication interface between a secure device and content player can be established. The invention allows content protection technology to be adapted and to maintain interoperability with existing technology used in present consumer equipment. In this manner backwards compatibility in content protection systems and secure device interfaces is obtained.

The invention will be further explained by reference to the drawings in which an embodiment of the systems of the invention applying the method of the invention are shown in a schematical manner.

Fig. 1 shows an in-home distribution network interconnecting a number of consumer content players.

Fig. 2 shows a diagram of the architecture of an embodiment of the system for providing encrypted data to be used in a content player according to the invention.

Fig. 3 shows a diagram of the architecture of an embodiment of the system for decrypting encrypted data in a content player according to the invention.

By way of example fig. 1 shows an in-home distribution netwerk 1 interconnecting a plurality of content player devices such as a TV set 2, a DVD player 3, a DVCR 4 and a PC 5. Further a camcorder 6, a set top box (STB) 7 and a secure device 8, such as for example a smart card, are connected to the network 1. Finally the network is linked to a wide area network, such as the internet, as indicated by reference nu-

CLAIMS

1. System for providing encrypted data to be used in a content player, comprising an encryption device for encrypting data using an encryption algorithm, a protection device for providing secure device data, and for providing information on a protocol for communication between the content player and a secure device, and a control device for providing a protected contents containing the encrypted data, the secure device data, said protocol information and attribute data on the different parts inside the protected contents, wherein <A>.

2. System according to claim 1, wherein said protection device provides at least one secure device applet containing said information on a protocol for communication.

3. System for decrypting encrypted data in a content player, comprising an input for receiving ~~encrypted data~~ protected contents containing encrypted ~~contents~~ data, secure device data, information on a protocol for communication between the content player and a secure device, and attribute data on the different parts inside the protected contents, a decryption device and a control device, wherein <A>, wherein the control device is programmed to use ~~said~~ (the attribute data to find the appropriate) protocol information to establish a communication interface between the decryption device and a secure device used with the content player, wherein the decryption device is adapted to communicate with the secure device as controlled by the protocol information to obtain information required to decrypt the encrypted data.

4. System according to claim 3, wherein said protocol information is provided as a secure device applet, whe-

rein the control device (16) is programmed to operate as a virtual machine to execute the secure device applet to establish said communication interface.

5. System according to claim 3, wherein at least one secure device applet in the protected contents is authenticated, wherein the control device (16) comprises an applet loader (19) for verifying the authentication of a secure device applet, wherein only a verified secure device applet is loaded into the virtual machine.

6. System according to claim 5, wherein at least one secure device applet in the protected contents is encrypted, wherein the applet loader (19) is adapted to decrypt an encrypted secure device applet.

7. System according to claim 4, 5 or 6, wherein the virtual machine comprises a content player application program interface and a security application program interface, the secure device applet communicating with the content player and the secure device by means of said interfaces.

8. System according to anyone of claims 4-7, wherein the control device (16) is arranged to determine the type of secure device (8) used in the system, wherein the control device (16) is arranged to retrieve a secure device applet from the protected contents corresponding with the determined type of secure device.

9. System according to anyone of claims 4-8, wherein the system is part of a content player (2-7) connected to a network (1), wherein the control device (16) is arranged to determine the type of secure device used in the system, and wherein the control device is arranged to request a corresponding secure device applet to be downloaded from a service provider.

10. Method for providing a communication interface between a decryption device (15) and a secure device (8) in a content player (2-7), comprising receiving a protected contents containing

information on a protocol for communication between the content player and a secure device, and attribute data on the different parts inside the protected contents, retrieving said protocol information from the protected contents to establish a communication interface between the decryption device and a secure device used with the contents player.

11. Method according to claim 10, wherein said protocol information is provided as a secure device applet, wherein the secure device applet is executed in a virtual machine to establish the communication interface.

12. Method according to claim 10 or 11, further comprising detecting the type of secure device used with the content player, and retrieving corresponding protocol information or a secure device applet from the protected contents.

13. Method according to claim 10 or 11, further comprising detecting the type of secure device used with the content player, and requesting corresponding protocol information or a secure device applet from a source providing the protected contents.

14. Method according to anyone of claims 10-13, wherein said protocol information or secure device applet is authenticated, further comprising verifying the authentication, and using only verified protocol information or a verified secure device applet to establish said communication interface.

~~15. Method for transmitting or the like encryted data obtained by means of a system according to claim 1 or 2,~~

FAX v. 6/11/00

Insert A, claims 1 and 3:

said secure device data comprises information required to decrypt the encrypted data, and wherein the attribute data comprises information to find in the protected contents the appropriate protocol for communication between the content player and the secure device for retrieving the information to decrypt the encrypted data

Insert B, claim 10:

the attribute data comprising information to find in the protected contents the appropriate protocol for communication between the content player and the secure device for retrieving the information to decrypt the encrypted data, and

Insert C, page 11, line 26:

15. Method for broadcasting protected contents, comprising encrypting data using an encryption algorithm, providing secure device data, providing information on a protocol for communication between a content player (2-7) and a secure device (8), providing protected contents containing the encrypted data, the secure device data, the protocol information and attribute data, and broadcasting the protected contents, wherein said secure device data comprises information required to decrypt the encrypted data, and wherein the attribute data comprises information to find in the protected contents the appropriate protocol for communication between the content player and the secure device for retrieving the information to decrypt the encrypted data.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 1/00 — A1

(11) International Publication Number: WO 00/13073

(43) International Publication Date: 9 March 2000 (09.03.00)

(21) International Application Number: PCT/EP99/06344

(22) International Filing Date: 30 August 1999 (30.08.99)

(30) Priority Data:
98202891.2 31 August 1998 (31.08.98) EP

(71) Applicant *(for all designated States except US)*: IRDETO ACCESS B.V. [NL/NL]; Jupiterstraat 42, NL-2132 HD Hoofddorp (NL).

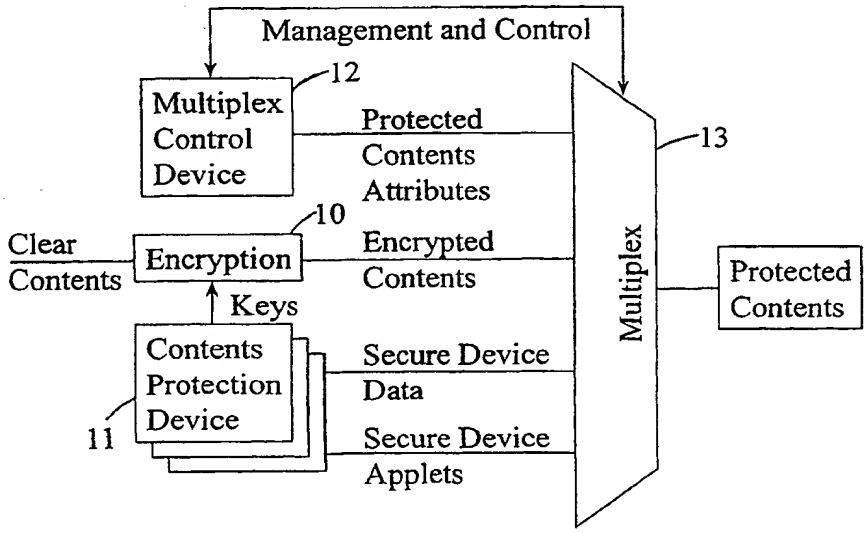
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: MOOIJ, Wilhelmus, Gerardus, Petrus [NL/NL]; Basilicum 7, NL-1115 DK Duivendrecht (NL). WAJS, Andrew, Augustine [GB/NL]; Schotersingel 93, NL-2023 AA Haarlem (NL).

(74) Agent: DE VRIES & METMAN B.V.; Gebouw Autumn, Overschiestraat 184 N, NL-1062 XK Amsterdam (NL).

(81) Designated States: CN, JP, US.

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SYSTEM FOR PROVIDING ENCRYPTED DATA, SYSTEM FOR DECRYPTING ENCRYPTED DATA AND METHOD FOR PROVIDING A COMMUNICATION INTERFACE IN SUCH A DECRYPTING SYSTEM



(57) Abstract

A system for providing encrypted data to be used in a content player, comprises an encryption device for encrypting data using an encryption algorithm, a protection device for providing security device data, and for providing information on a protocol for communication between the content player and a secure device, and a control device for providing protected contents containing the encrypted data, the secure device data, said protocol information and attribute data on the different parts inside the protected contents. The encrypted data can be transmitted or stored on a suitable medium.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

System for providing encrypted data, system for decrypting encrypted data and method for providing a communication interface in such a decrypting system.

The invention generally relates to a system for providing encrypted data to be used in a content player, to a system for decrypting encrypted data in a content player, and to a method for providing a communication interface between a decryption device and a secure device in a content player. More particularly the invention relates to such systems and a method to create an open access interface for a wide range of multimedia terminals.

In the present specification the term "content player" is meant to indicate any type of consumer equipment, such as a (digital) TV set, a set top box, a DVD player or a (digital) VCR. In order to allow access to contents, such as a movie, football match, etc., it is known to protect the contents by encryption of the data using a suitable encryption algorithm. Subscribers are provided with a set top box for example and a secure device, wherein the secure device generates information necessary to decrypt the encrypted data. Conventional systems of this type are provided with a fixed interface and protocols for communication between the secure device and the content player. A fixed interface shows the disadvantage that the content player can only be used with one or more specific secure devices.

The invention aims to provide systems and a method of the above-mentioned type allowing to create a variable interface between the secure device and a content player.

According to a first aspect of the invention, a system for providing encrypted data to be used in the content

player is provided, comprising an encryption device for encrypting data using an encryption algorithm, a protection device for providing secure device data, and for providing information on a protocol for communication between the content player and a secure device, and a control device for providing a protected contents containing the encrypted data, the secure device data, said protocol information and attribute data on the different parts inside the protected contents.

According to a second aspect of the invention, a system for decrypting encrypted data in a content player is provided, comprising an input for receiving a protected contents containing the encrypted data, secure device data, information on a protocol for communication between the content player and a secure device, and attribute data on the different parts inside the protected contents, a decryption device and a control device, wherein the control device is programmed to use said protocol information to establish a communication interface between the decryption device and a secure device used with the contents player, wherein the decryption device is adapted to communicate with the secure device as controlled by the protocol information to obtain information required to decrypt the encrypted data.

According to a further aspect of the invention, a method for providing a communication interface between a decryption device in a content player and a secure device is provided, comprising receiving a protected contents containing information on a protocol for communication between the content player and a secure device, and attribute data on the different parts inside the protected contents, retrieving said protocol information from the protected contents to establish a communication interface between the decryption device and a secure device used with the contents player.

According to a still further aspect of the invention a method for transmitting or the like of encrypted data is provided, wherein the encrypted data is obtained by means of the system for providing encrypted data according to the invention.

In this manner the invention provides a variable interface platform, wherein any communication interface between a secure device and content player can be established. The invention allows content protection technology to be adapted and to maintain interoperability with existing technology used in present consumer equipment. In this manner backwards compatibility in content protection systems and secure device interfaces is obtained.

The invention will be further explained by reference to the drawings in which an embodiment of the systems of the invention applying the method of the invention are shown in a schematical manner.

Fig. 1 shows an in-home distribution network interconnecting a number of consumer content players.

Fig. 2 shows a diagram of the architecture of an embodiment of the system for providing encrypted data to be used in a content player according to the invention.

Fig. 3 shows a diagram of the architecture of an embodiment of the system for decrypting encrypted data in a content player according to the invention.

By way of example fig. 1 shows an in-home distribution netwerk 1 interconnecting a plurality of content player devices such as a TV set 2, a DVD player 3, a DVCR 4 and a PC 5. Further a camcorder 6, a set top box (STB) 7 and a secure device 8, such as for example a smart card, are connected to the network 1. Finally the network is linked to a wide area network, such as the internet, as indicated by reference nu-

meral 9. In this example of an in-home distribution network 1, the STB 7 and the secure device 8 communicate through a communication interface in order to decrypt any encrypted data obtained from protected contents as will be described later. The STB 7 and secure device 8 are common to the content players 2-5 in this example, although it is also possible that each of the content players is provided with its own decoder/decryption device communicating with its own secure device. It is noted that protected contents can be moved through the network 1 to a target content player using a suitable protocol and adressing technique which are not part of the present invention.

Fig. 2 shows a system for providing encrypted data to be used in a content player, comprising an encryption device 10, a protection device 11 and a control device 12 including a multiplexer 13. Clear contents, such as a movie, a football match, etc., is encrypted in the encryption device 10 using a suitable encryption algorithm. In the encryption algorithm keys are used which are provided by the protection device 11 and these keys are themselves encrypted in one or more formats by the protection device 11. The encrypted keys are provided as secure device data. The protection device 11 further provides information on a protocol for communication between the content player and the secure device 8. In the embodiment shown, the information on the protocol and encryption format(s) is provided as one or more secure device applets.

The encrypted contents provided by the encryption device, the secure device applet(s) and the secure device data are multiplexed into protected contents, also containing attribute data provided by the control device 12. The attribute data are required to find the relevant parts inside the

protected contents structure. The output of the multiplexer 13 can be broadcast for example or stored on a suitable medium for later use.

The system shown in fig. 2 may be adapted to handle one or more different secure device formats and for each of these formats the protection device 11 provides a secure device applet. The main funtion of the secure device applet is to implement in the content player the protocol and format to communicate with the secure device connected to the content player. In this manner it is possible to provide an interface between the secure device and the content player without specific knowledge beforehand of the protocol required by the specific secure device used.

Preferably each secure device applet is authenticated, for example by a signature which shows that it originated from a legitimate source. Suitable public key cryptographic hashing functions can be used.

Fig. 3 shows a system for decrypting encrypted data in a content player as shown, comprising an input 14 for receiving protected contents, a decryption device 15 and a control device 16 including a demultiplexer 17. A secure device 8 is connected to the control device 16. Further a decoder 18 is shown for decoding decrypted data in a manner known per se. The decoder 18 is not part of the present invention. The attribute data is used in the control device 16 to demultiplex the protected contents to retrieve a secure device applet or applets, the secure device data and the encrypted contents and to forward the respective parts of the contents to the corresponding components of the content player.

In order to decrypt the encrypted contents, the content player needs to retrieve the keys from the secure device 8. To this end the control device 16 determines the type

of secure device 8 connected to the content player and searches the attribute data to select the appropriate corresponding security device applet. The control device 16 includes an applet loader 19 to verify the signature of the secure device applet. If the secure device applet is verified, this applet is downloaded in a virtual machine programmed into the control device and is executed in this environment to establish a communication interface between the secure device 8 and the content player and decryption device 15. Once the communication interface is established, the secure device applet operates to fetch the secure device data from the protected contents which is tranformed by the secure device 8 into the keys required by the decryption device 15 to decrypt the encrypted contents.

As noted, the applet loader 19 verifies whether the secure device applet is an authentic one. In this manner the applet loader restricts access to the virtual machine to those applets originating from an authentic source. A standard method to achieve verifying of the secure device applet is authentication using a public key cryptographic hashing function. Optionally, the applet may be encrypted using a conventional secret key cryptographic algorithm. The attribute data contains fields specifying both the type of cryptographic algorithm and secret key index to be used in the signature verification process.

In the virtual machine, the secure device applet uses a content player application program interface to communicate with the content player on the one side and a security application program interface to communicate with the secure device 8 and the decryption device 15.

The control device 12 is arranged to indicate in the attribute data the type of secure device 8 supported in

the content player. When the secure device 8 has been determined, for example by finding the unique identifier in a manner known per se, the secure device applet corresponding with the secure device by virtue of having a matching identifier is selected from the attribute data. On the basis of this information, the applet loader retrieves the secure device applet from the protected contents. This process will generally be used in an application, wherein the protected contents is received in a continuous stream in case of a broadcasting environment for example. The same process can be used when the protected contents is stored on a tape or disc. In case of an broadcasting environment or wide area network, it is also possible for the applet loader 19 to request a service provider or the like to forward a secure device applet corresponding to the detected type of secure device.

It is observed that the security of the system described is at least as good as any existing security system. As the protected contents is always encrypted until it reaches the target content player, it is difficult to obtain a clear text version of the contents. Moreover the flexibility of the system described allows for defense and counter measures against presently existing attacking techniques, which counter measures are not available in existing protection systems.

It is noted that the term "content player" should be understood as to mean any device mentioned above or even a separate decoder equipment having an interface for the secure device. Further it is noted that although wording is used in the above description suggesting separate devices in the systems decribed, it will be clear that both the encrypting and decrypting system can be implemented by means of a micropro-

cessor and suitable peripheral circuits operating in the manner described as controlled by suitable software.

The system described supports a wide range of applications. As already mentioned, a first application area is a broadcasting environment. The content player in this case can be a set top box connected to a TV or a DVCR. The virtual machine can be implemented using JAVA. Generally an ISO 7816 smart card is used as secure device. According to a favourable embodiment, it will also be possible for non-subscribers to buy a specific "event", such as a football match, using a standard banking card, wherein the applet loader requests the service provider to download a suitable secure device applet. Other applications are pre-recorded media, such as CD, DVD, DVCR tapes and other cassettes. In the described system of the invention, the stored protected contents includes a number of supported secure device applets, so that the applet loader of the control device can retrieve the secure device applet corresponding with the secure device used in the specific content player. In this manner again backwards compatibility is allowed, whereas future upgrades can be made in a flexible manner.

The invention is not restricted to the above-described embodiments which can be varied in a number of ways within the scope of the following claims.

CLAIMS

1. System for providing encrypted data to be used in a content player, comprising an encryption device for encrypting data using an encryption algorithm, a protection device for providing secure device data, and for providing information on a protocol for communication between the content player and a secure device, and a control device for providing a protected contents containing the encrypted data, the secure device data, said protocol information and attribute data on the different parts inside the protected contents.

2. System according to claim 1, wherein said protection device provides at least one secure device applet containing said information on a protocol for communication.

3. System for decrypting encrypted data in a content player, comprising an input for receiving encrypted data containing encrypted contents, secure device data, information on a protocol for communication between the content player and a secure device, and attribute data on the different parts inside the protected contents, a decryption device and a control device, wherein the control device is programmed to use said protocol information to establish a communication interface between the decryption device and a secure device used with the content player, wherein the decryption device is adapted to communicate with the secure device as controlled by the protocol information to obtain information required to decrypt the encrypted data.

4. System according to claim 3, wherein said protocol information is provided as a secure device applet, whe-

rein the control device is programmed to operate as a virtual machine to execute the secure device applet to establish said communication interface.

5. System according to claim 3, wherein at least one secure device applet in the protected contents is authenticated, wherein the control device comprises an applet loader for verifying the authentication of a secure device applet, wherein only a verified secure device applet is loaded into the virtual machine.

6. System according to claim 5, wherein at least one secure device applet in the protected contents is encrypted, wherein the applet loader is adapted to decrypt an encrypted secure device applet.

7. System according to claim 4, 5 or 6, wherein the virtual machine comprises a content player application program interface and a security application program interface, the secure device applet communicating with the content player and the secure device by means of said interfaces.

8. System according to anyone of claims 4-7, wherein the control device is arranged to determine the type of secure device used in the system, wherein the control device is arranged to retrieve a secure device applet from the protected contents corresponding with the type of secure device.

9. System according to anyone of claims 4-8, wherein the system is part of a content player connected to a network, wherein the control device is arranged to determine the type of secure device used in the system, and wherein the control device is arranged to request a corresponding secure device applet to be downloaded from a service provider.

10. Method for providing a communication interface between a decryption device and a secure device in a content player, comprising receiving a protected contents containing

information on a protocol for communication between the content player and a secure device, and attribute data on the different parts inside the protected contents, retrieving said protocol information from the protected contents to establish a communication interface between the decryption device and a secure device used with the contents player.

11. Method according to claim 10, wherein said protocol information is provided as a secure device applet, wherein the secure device applet is executed in a virtual machine to establish the communication interface.

12. Method according to claim 10 or 11, further comprising detecting the type of secure device used with the content player, and retrieving corresponding protocol information or a secure device applet from the protected contents.

13. Method according to claim 10 or 11, further comprising detecting the type of secure device used with the content player, and requesting corresponding protocol information or a secure device applet from a source providing the protected contents.

14. Method according to anyone of claims 10-13, wherein said protocol information or secure device applet is authenticated, further comprising verifying the authentication, and using only verified protocol information or a verified secure device applet to establish said communication interface.

15. Method for transmitting or the like encryted data obtained by means of a system according to claim 1 or 2.

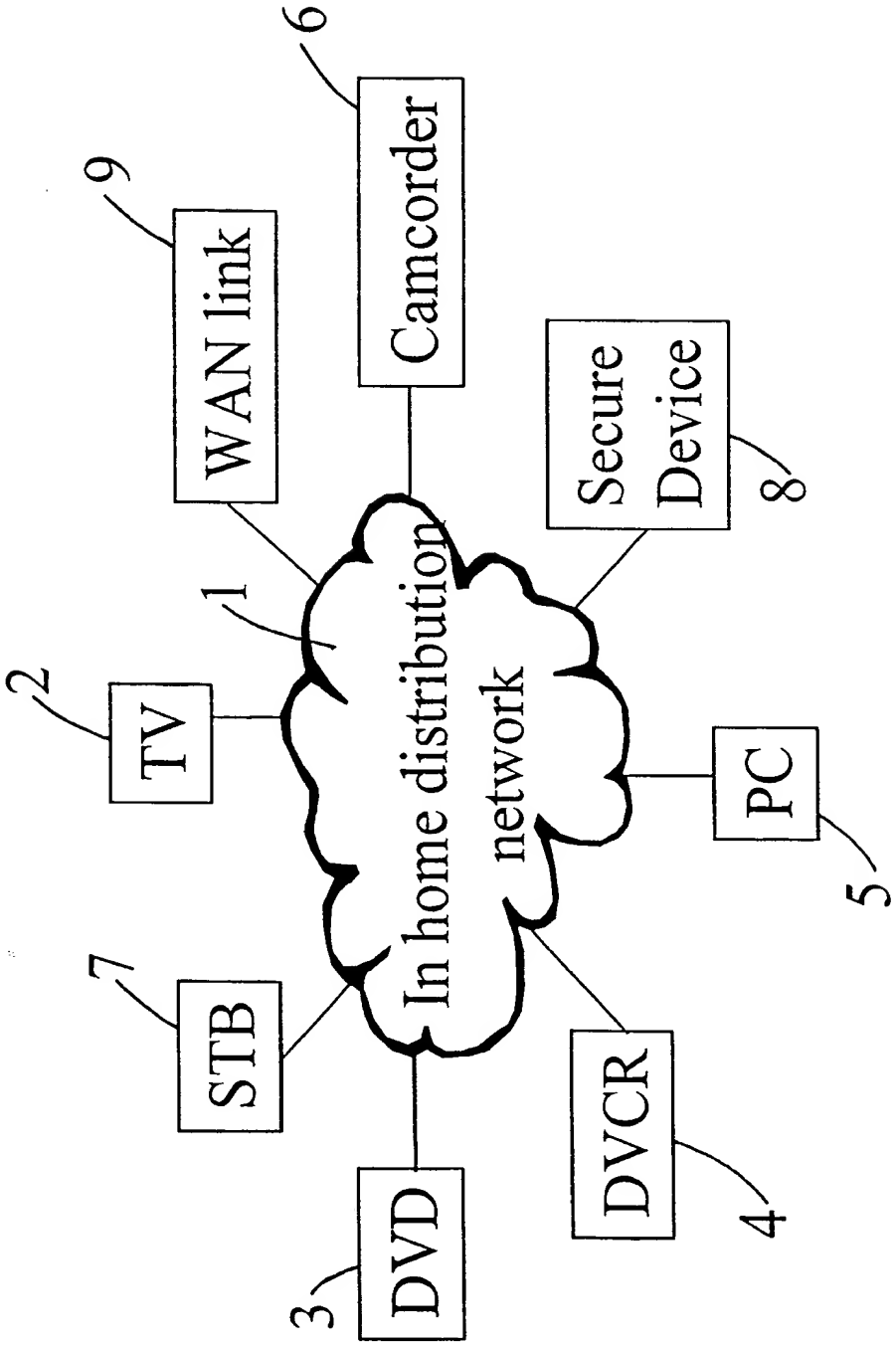

In home distribution network
1
WAN link
9
Camcorder
6
Secure Device
8
TV
2
PC
5
STB
7
DVCR
4
DVD
3

Fig. 1

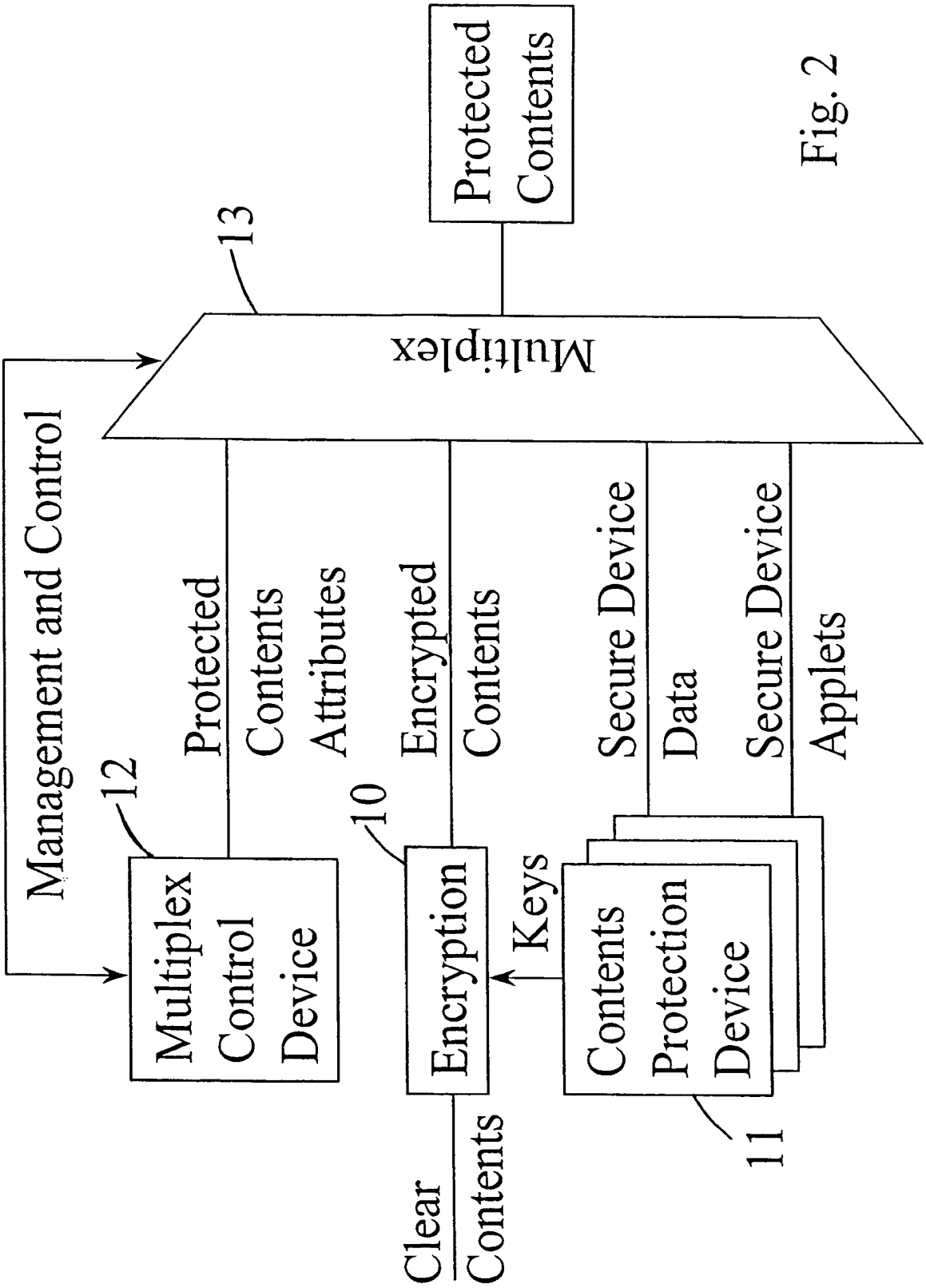

Protected Contents
13
Multiplex
Management and Control
Protected Contents Attributes
Encrypted Contents
Secure Device Data
Secure Device Applets
12
10
Multiplex Control Device
Encryption
Keys
Contents Protection Device
11
Clear Contents

Fig. 2

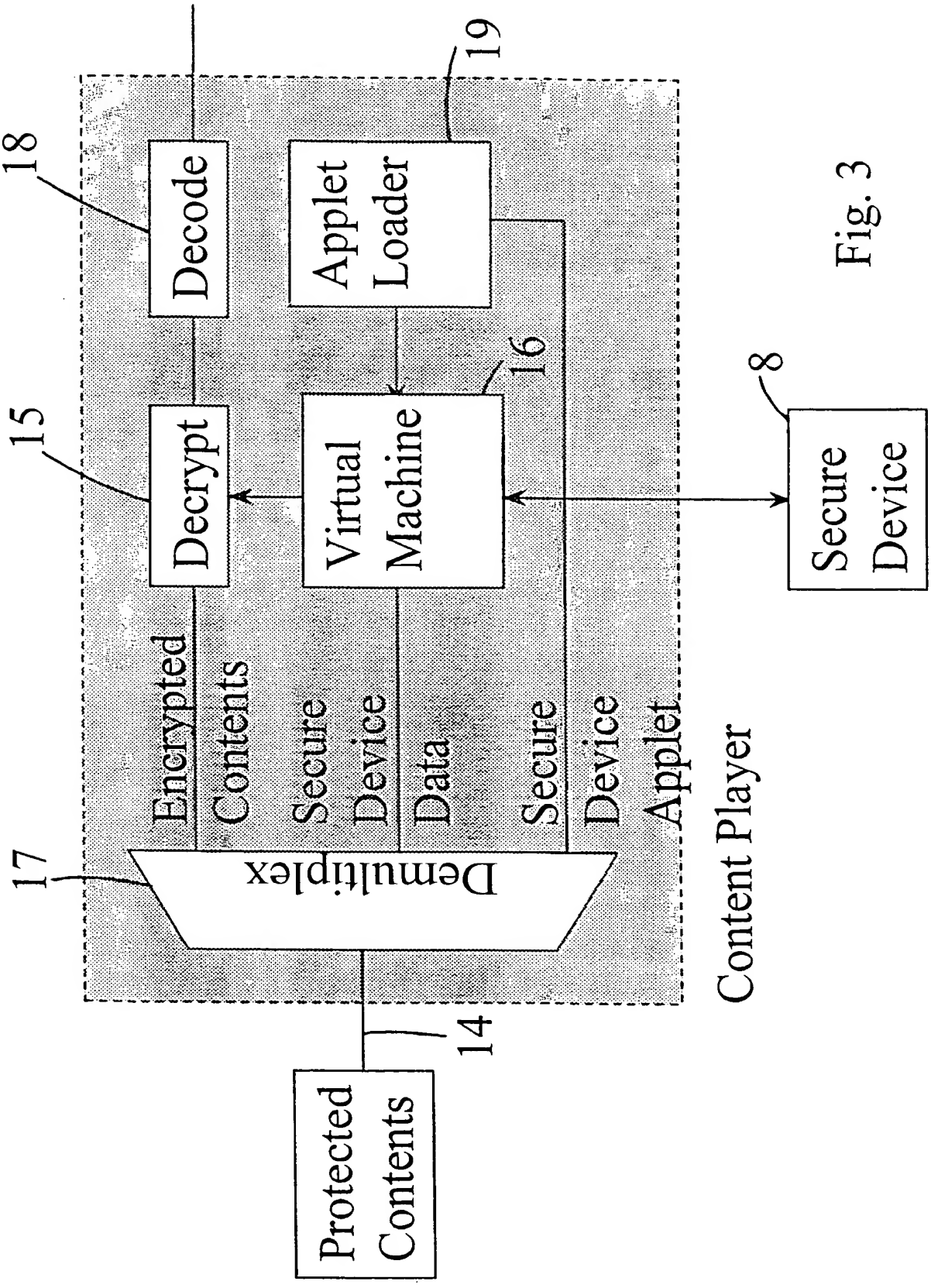

Protected Contents
14
Content Player
Demultiplex
17
Encrypted Contents
Secure Device Data
Secure Device Applet
Decrypt
15
Virtual Machine
16
Decode
18
Applet Loader
19
Secure Device
8

Fig. 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 99/06344

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 679 980 A (IBM) 2 November 1995 (1995-11-02) figures 1-7,12-24 figures 30-35 column 8, line 8 -column 13, line 47 column 19, line 19 -column 25, line 5 column 29, line 32 -column 36, line 27	1-6, 8-10,14, 15
X	US 5 630 057 A (HAIT JOHN N) 13 May 1997 (1997-05-13) figures 1,3 column 14, line 37 - line 59 column 15, line 44 -column 18, line 11	1-8, 10-15

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 January 2000	14/01/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Weiss, P

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

...formation on patent family members

...nal Application No
PCT/EP 99/06344

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0679980 A	02-11-1995	US 5757907 A	26-05-1998
		BR 9501522 A	21-11-1995
		CA 2145926 A,C	26-10-1995
		JP 7295801 A	10-11-1995
US 5630057 A	13-05-1997	US 5581763 A	03-12-1996
		AU 3840689 A	12-01-1990
		EP 0382811 A	22-08-1990
		WO 8912864 A	28-12-1989